



XKEYSCORE for Counter-CNE

"Using the XKS CNE dataset and a DISGRUNTLEDDUCK fingerprint, we now see at least 21 TAO boxes with evidence of this intrusion set, most of which are associated with projects aimed at Iran WMD targets." -- MHS, July 2010

March, 2011


xks-cne@r1.r.nsa



Overall Classification

The overall classification of this presentation is:

TOP SECRET//COMINT//REL TO USA, FVEY



What is XKEYSCORE?

- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends



What is XKEYSCORE?

- A suite of software running on a Linux host
- *Classically*, used for DNI processing, selection and survey
- A distributed hierarchy of servers at field sites and headquarters
 - Extract and tag metadata & content from traffic
 - Servicing analyst queries and workflows
- Web and programmatic front-ends

TOP SECRET//COMINT//REL TO USA, FVEY

XKEYSCORE GUI



XK Metaviewer: shared by f610065:Category Hits at 67D - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.nsa.ic.gov:8143/XKEYSCORE/search/standardsearchformmysearchHome.do wp Ethernet

ESS1377: SIDToday for 1/24/... Ethernet - Wikipedia, the free... My Signatures XK Metaviewer: shared by f610065:Category Hits XKEYSCORE - For Analysts...

The system is audited to USF D-18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE Welcome [redacted] Log Out

Home Admin Users Search Workflow Centre Results Fingerprints Statistics Map My Account XKI drum Help

Navigation Filter

- Search Wizard
- CNF
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Keylogger
 - Machine Information
 - Network Information
 - Registry
- Classic
 - MultiSearch
 - Classic AM
 - Art
 - BlackBerry
 - Call Logs
 - Category DNI
 - Cellular DNI
 - Circled Passwords
 - Cleartext
 - DNS
 - Document Metadata
 - Document Tagging
 - Email Addresses
 - Extracted Files
 - Full Log DNI
 - Gen Info
 - HTTP Activity
 - KE Parser
 - Keylogger
 - Logins and Passwords

Histogram Grid

Page 1 of 1 Clear Selection Export

Filter Filter Count

2304 1/4

shared by f610065:Category Hits

Help Actions Reports View Map View FILTERS

From	Sigad	Active User	Case/Location	From IP	To IP	From Port	To Port	From Country (I)	From City (IP)	From Latitude (I)	From Longitude (I)	To Country (I)	To City (IP)	To Latitude
IFT/001	US-967D		UA2AA00CD	57	57	2304	2631	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
ILIT/001	US-967D		UA2AA00CB	57	57	2304	3390	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1653	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IFT/001	US-967D		UA2AA00CD	57	57	2304	1130	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1679	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
ILIT/001	US-967D		UA2AA00CB	57	57	2304	2580	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	3190	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
ILIT/001	US-967D		UA2AA00CB	57	57	2304	1120	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IFT/001	US-967D		UA2AA00CD	57	57	2304	1600	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1603	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
ILIT/001	US-967D		UA2AA00CB	57	57	2304	3050	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88
IETT/001	US-967D		UA2AA00CB	57	57	2304	1083	FR	NEUILLYSUF	48.88	2.27	FR	NEUILLYSUF	48.88

Page 1 of 6 Page Size: 20 (Max: 100 rows per page) Displaying 1 - 20 of 174

saved: 80219757060313

The system is audited to USF D-18 and Human Rights Act compliance
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

TOP SECRET//COMINT//REL TO USA, FVEY



Example Search

- Let's try a search for suspicious stuff...

http_activity search, 5-eyes defeat, look for fingerprints:

`ndist/discovery/heuristic/BHAM/get_with_content` or `http/get/with_content`

- While the search runs, some gotchas:
 - You choose where your query is run
 - Content and metadata age-off
 - Burden is on user/auditor to comply with USSID-18 or other rules
 - Geolocation based on IP



Search Results

XX Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

ic.gov https://xks-central.corp.nsa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&rowUrl=%2F

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

X-KEYSCORE C2C Session Viewer

Session 15 of 17

Date/Time	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-11 13:47:44	3-411846/080000	192.168.1.100 (Private Address)	10.10.10.10 (Private Address)	43070	12468	ICP	224

Session Headers (0) Meta (7) Attachments (1)

Formatter: ASCII Send to: Download Session - Mode: Snippet Options - Search Content: Enter text to search

Quick Clicks

- Session
- Attachments
 - unknown
 - lex
 - unknown_515.x-ww
- One-Click Searches
 - Find fingerprint
 - ndis/discovery/headers
 - http/get/with_content
 - ndis/discovery/headers
 - Find traffic on
 - 192.168.1.100
 - 10.10.10.10
 - Find application
 - http/get/x-www-form-urlencoded
 - Find proxy hash
 - 0d0c20f7
 - Find opposite side of session
 - 192.168.1.100
 - 10.10.10.10

```

GET /?CAVIT HTTP/1.0
User-Agent: 625D1C33CF68DA7333FD3C02702E7BD2
Accept: */*
Host: 10.10.10.10:12468
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive

Reset from local: (1231) seq = 2661134980
  
```

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Done

Notes:

- Strange User-Agent
 - Probably NOT CNE but definitely something non-standard
 - Content: maybe a HTTP tunnel for some weird protocol?
- Reset from local...
- Should we write a Fingerprint?



Fingerprints and Appids

- Useful for identifying classes of traffic or particular targets (for SIGDEV or collection):
 - `mail/webmail/yahoo`
 - `browser/cellphone/blackberry`
 - `topic/s2B/chinese_missile`
- appid – a contest, highest scoring appid wins
- fingerprint – many fingerprints per session
- microplugin – a fingerprint or appid that is relatively complex (e.g. extracts and databases metadata)



Fingerprints and Appids (more)

- Written in language called "GENESIS" (go genesis-language):

```
appid('encyclopedia/wikipedia', 2.0) =  
  http_host('wikipedia' or 'wikimedia');  
fingerprint('dns/malware/MalwareDomains') =  
  dns_host('erofreex.info' or 'datayakoz.info'  
  or 'erogirlx.info' or 'pornero.info' or ...
```

- If a fingerprint contains a schema definition, a search form automatically appears in the XKEYSCORE GUI
- Power users can drop in to C++ to express themselves



More about searches

- Many different searches
 - Base search is Full Log DNI
 - Depending on traffic type, will generate searchable results for (example):

HTTP Activity	Network Information	GEO Info
Extracted Files	Email Addresses	Registry
Logins and Passwords	Document Metadata	Machine Info

- workflow – a user query that is run automatically usually every 24 hours



XKEYSCORE Gotchas

- Not all sites run latest XKEYSCORE software or fingerprints
- fingerprint submission:
 - XKEYSCORE team weighs mission-worthiness of user fingerprints vs computational cost
- Content and metadata ageoff

XKEYSCORE CNE



- Lots of endpoint data flows into XKS
TAO (no ECIs), GCHQ (almost all)
- Other limited flows include SIGINT
Forensics Center, TAO STAT
- XKEYSCORE works well for endpoint data
- Sometimes the paradigm breaks (e.g.
collected browser history file)

XKEYSCORE CNE (more)



- Payload types:
dirwalk, extracted file, system survey, network config, captured credentials, registry query, key logger, etc.
- Labeled `dnt_payload` in appid/fingerprint ontology
- Let's look at some DANDERSPRITZ data...

XKEYSCORE CNE (more)



XX Session Viewer - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xks-central.corp.usa.ic.gov:8443/XKEYSCORE/layouts/popOutLayout.jsp?pageTitle=Session Viewer&showUrl=%2FXKEYSCORE%2F%2FmetaViewer!

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

X-KEYSCORE C2C Session Viewer

Session: 50 of 703

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol	Length
2011-04-12 02:06:12	CC:WU00CAACDTD						10074

Session Header (3) Meta (4)

Format: LNT_PAYLOAD Send to: Down load Session Mode: Snippet Use one Search Content: enter text to search Clear

Quick Clicks

- Session
- One-Click Searches
 - Find fingerprint
 - extrin/experimental/process
 - Find traffic.cn
 - Find application
 - dnt_payload/processlist
 - Find opposite side of session
 - C.S.

PAYLOAD XML

```
<Process creationTime="2011-04-05T00:37:09.031250000" description="Initial" pid="460" ppid="532">lsass.exe</Process>
<Process creationTime="2011-04-05T00:37:11.72343750000" description="Initial" pid="655" ppid="140">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:13.781250000" description="Initial" pid="723" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:35.559575000" description="Initial" pid="792" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:36.484375000" description="Initial" pid="844" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:40.703125000" description="Initial" pid="860" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:41.500525000" description="Initial" pid="895" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:42.718750000" description="Initial" pid="965" ppid="140">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:54.281250000" description="Initial" pid="1340" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:54.640525000" description="Initial" pid="1348" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:57.171375000" description="Initial" pid="1452" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:57.710750000" description="Initial" pid="1500" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:37:58.046375000" description="Initial" pid="1532" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:00.625300000" description="Initial" pid="1538" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:00.750300000" description="Initial" pid="1630" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:01.234375000" description="Initial" pid="1620" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:01.421375000" description="Initial" pid="1642" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.125300000" description="Initial" pid="1672" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.500300000" description="Initial" pid="1690" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:02.625300000" description="Initial" pid="1720" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:08.046375000" description="Initial" pid="1832" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:08.437500000" description="Initial" pid="1932" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:14.562500000" description="Initial" pid="2216" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:17.4.671375000" description="Initial" pid="2240" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:17.625300000" description="Initial" pid="2350" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:38:23.031250000" description="Initial" pid="2620" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:47.108340500" description="Initial" pid="1638" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:48.672375000" description="Initial" pid="1756" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:54.681375000" description="Initial" pid="2092" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:45:57.839375000" description="Initial" pid="2888" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:46:00.750750000" description="Initial" pid="2956" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:46:02.203303200" description="Initial" pid="755" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:46:06.075397000" description="Initial" pid="452" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:46:15.408522600" description="Initial" pid="3530" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:51:23.533589300" description="Initial" pid="3230" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-05T00:56:53.997113900" description="Initial" pid="4030" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:26:03.260310500" description="Initial" pid="3426" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:26:03.476365500" description="Initial" pid="5136" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:29:30.503950000" description="Initial" pid="5440" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:29:39.660251000" description="Initial" pid="5430" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:39:00.453215000" description="Initial" pid="363" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:39:00.609170000" description="Initial" pid="135" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:48:36.768533500" description="Initial" pid="4656" ppid="440">svchost.exe</Process>
<Process creationTime="2011-04-11T22:48:36.956375000" description="Initial" pid="2572" ppid="440">svchost.exe</Process>
```

This system is audited for USSID 18 and Human Rights Act compliance
CLASSIFICATION: TOP SECRET//COMINT//REL TO USA, AUS, CAN, GDR, NZL

Done

XKEYSCORE CNE (more)



- Recent Developments
 - Upgrade of XKEYSCORE CNE
 - Keyloggers: keylogger/perfect/extension
 - PCAP Reingestion
- Router Redirection



Counter CNE Methodology

(refer to Counter CNE Resources slide...)

- Hypothesis/research-driven
 - "Could South Korean CNE be using similar selectors to FVEY CNE?"
 - "What keywords could be used to find keyloggers ("example: keylog OR keystroke")
- Bogus or Unusual Traffic
 - HTTP GET with content (example in this presentation)
 - HTTP POST at odd hours (from Russia 0200-0359Z)
 - Funky user agents
- Known-Host or User driven (e.g. drop sites)
- XKEYSCORE is GOOD at these kinds of things



CNE-Specific

- Registry searches (e.g. SIMBAR)
- Fused Active/Passive search
 - common selectors
 - document hashes
- Known Processes (malicious executables or code)
 - ... Let's enhance the process list appid
- map-reduce within CNE cluster using GENESIS calls



XKEYSCORE Doesn't Do...

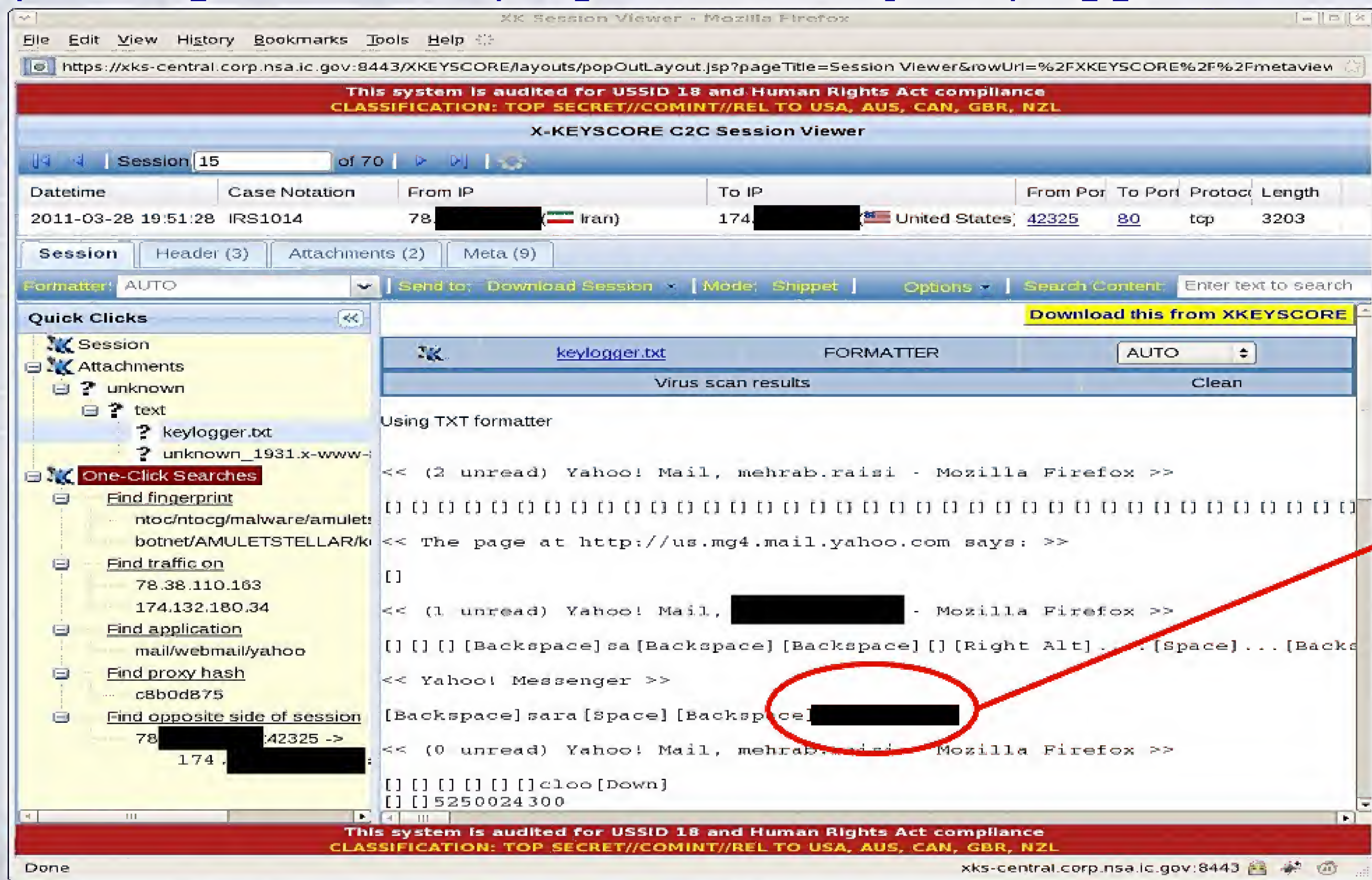
- ... at all (well, automatically, anyways)
 - Paired traffic heuristic-based approach
 - HTTP[S] imbalance (e.g. GET without response)
 - IP/DNS mismatch*
- ... on an automatic basis
 - Network or host characterization
 - Changes in IP/DNS mapping over time
 - Changes over time in malware comms



Counter CNE Resources

- *How to Discover Intrusions [using XKEYSCORE]* by [REDACTED] and [REDACTED] (paper)
- MHS INDEX – Foreign CNE Discovery Page
https://wiki.itd.nsa/wiki/Foreign_CNE_Discovery
- CSEC and GCHQ – DONUT (unknown protocols):
<https://tiso.sigint.cse/snipehunt/index.php/DONUT>
- GCHQ Discovery Posted some Research of Detecting Man-on-the-Side Attacks:
<https://tiso.sigint.cse/snipehunt/index.php/MOTS>
- GCQH Disco Team posts POC's for different Intrusions and some Details:
<https://wiki.gchq/index.php/Discovery>
- The GCHQ DISCO team also posts Discovery Theories they run once a week:
https://wiki.gchq/index.php/Discovery_Afternoons
- XKEYSCORE Fingerprints

Using TAO-obtained Iranian implant encryption keys, inline decrypt using XKS microplugin – IRGC-QF keylogger data!





Points of Contact

- MHS Index Team

[REDACTED] : [REDACTED]@nsa.ic.gov

- CES/TRANGRESSION

[REDACTED] : [REDACTED]@nsa.ic.gov

[REDACTED] : [REDACTED]@nsa.ic.gov

- NSA/Countering Foreign Intelligence

[REDACTED] : [REDACTED]@nsa.ic.gov

- NTOC ??

- XKEYSCORE

[REDACTED], [REDACTED] : xks-cne@r1.r.nsa